High Speed Security for Servers

Name: Dan Eakins

Title: Senior Product Line Manager

Company: Broadcom Security Line of Business

San Jose January 23-24, 2001 • Taipei February 14-15, 2001

Agenda

- Cryptography Processing Cycle
- Security Models and Background
- The Security Bottleneck
- Pushing VPN performance
- Pushing SSL Performance
- Future Solutions

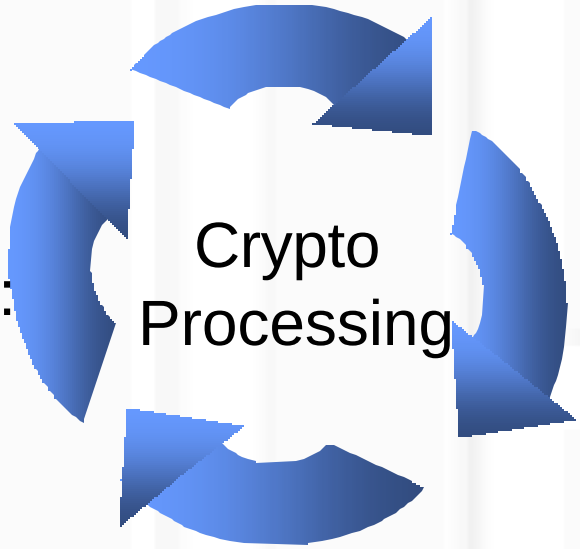
Cryptography Processing Cycle

Increasing needs for Cryptography Processing

- **Stronger Ciphers**
- **eCommerce**
- **Remote office VPNs**
- **B2B**

New Applications (e.g.):
- Email
- File Transfer

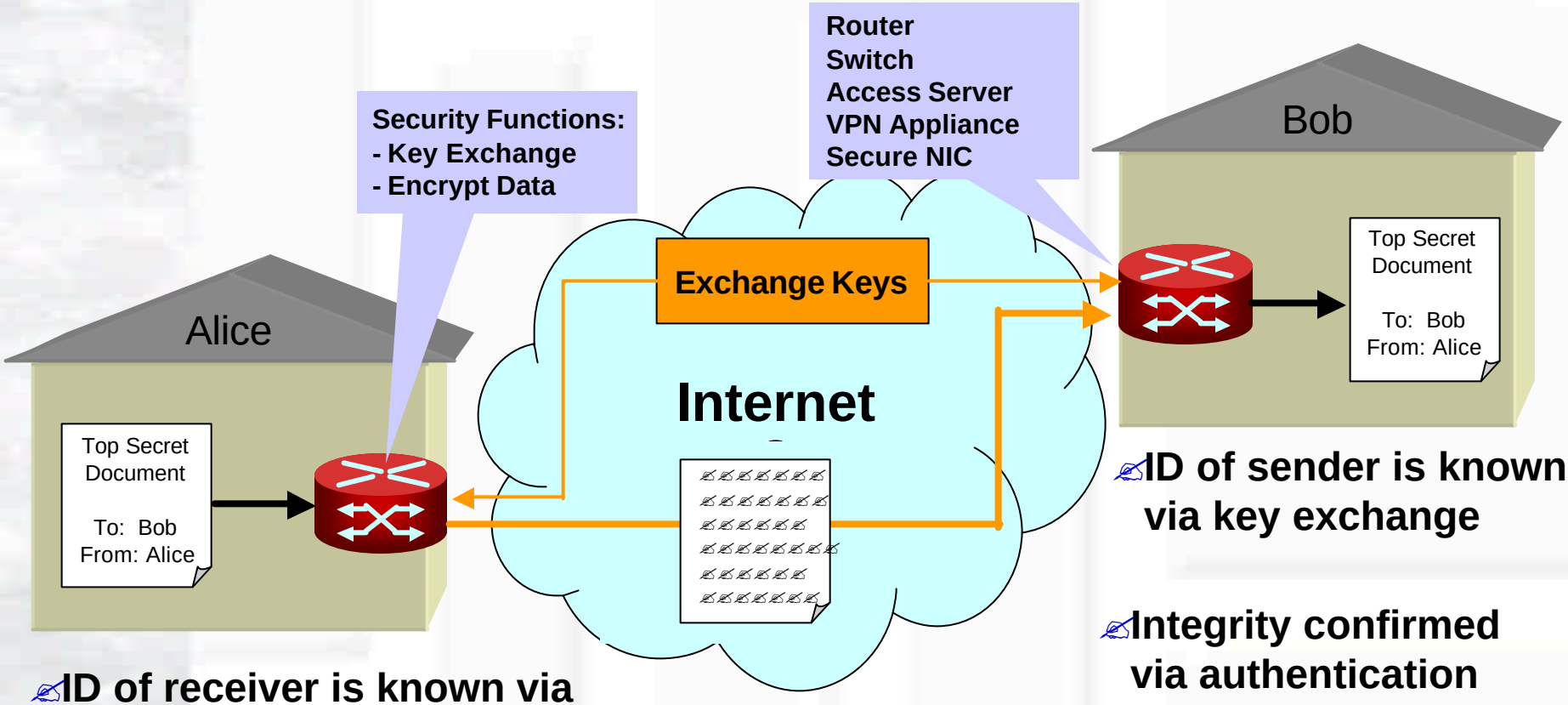
Increase Crypto Processing



Increases in:
- Bandwidth
- Internet Use
-Cipher Lengths

Increase Crypto Processing

Secure Exchange of Data



- ID of receiver is known via key exchange
- Data is confidential via encryption
- ID of sender is known via key exchange
- Integrity confirmed via authentication

Platform Conference

BROADCOM.

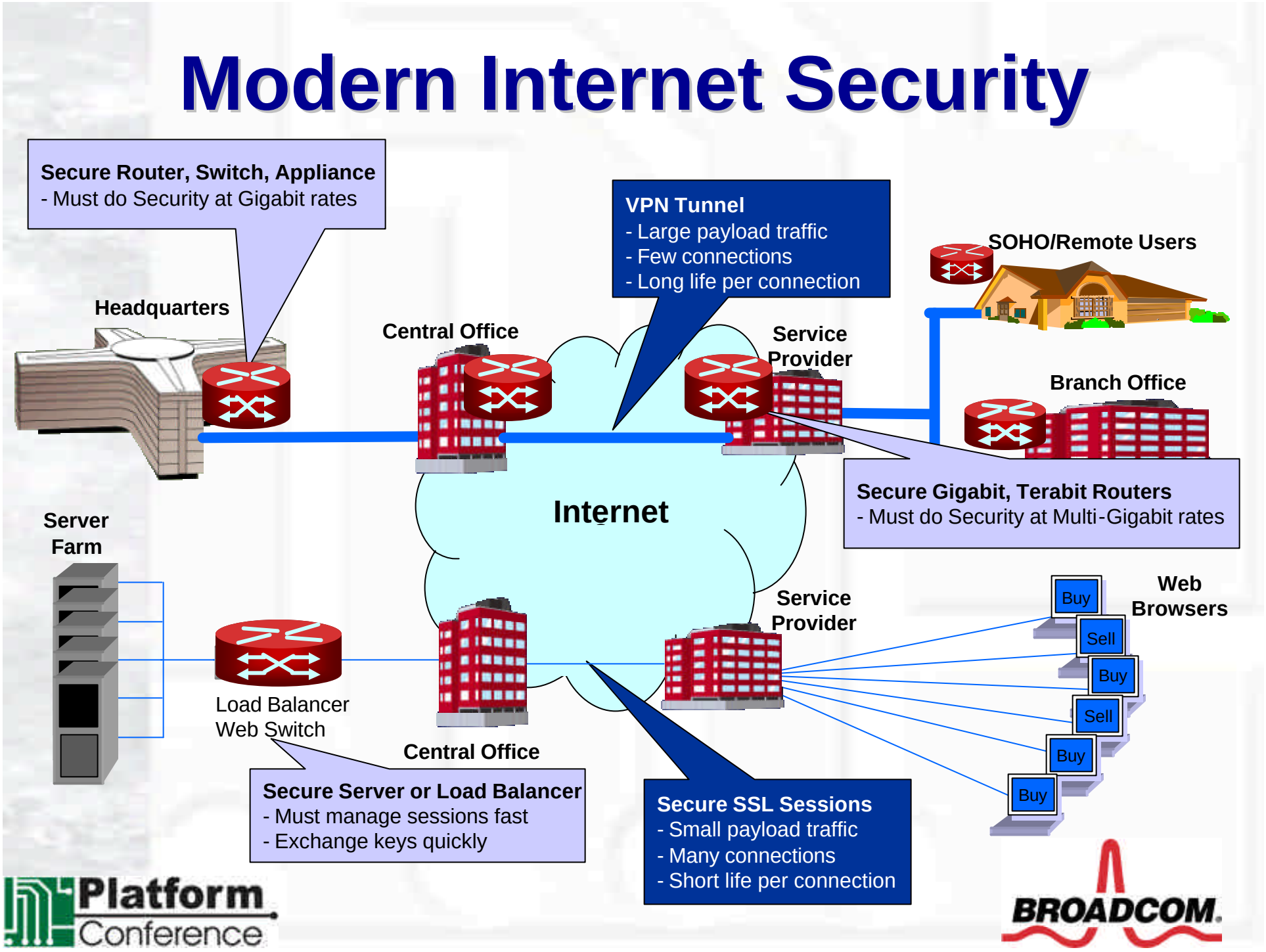
IPSec & IKE

- Internet Protocol Layer Standard Defining a Method of Using Public Network Infrastructure for Secure Networking
- Predominant Standard Being used to Implement Virtual Private Networks (VPN)
- Defines encryption Algorithms (DES, 3DES, RC4) and Authentication Algorithms (MD5, SHA-1) to be Used
- Defines Public Key Exchange to Use (Diffie-Hellman)

SSL

- Higher Layer Protocol used Predominately to Secure Web Traffic
  - Used in web browsers (Netscape, Explorer)
  - Software implementations are effective
  - TLS (Transport Layer Security) is next generation of SSL
- Predominant Standard Being used for E-Commerce
- Defines Encryption Algorithms (RC4) and Authentication Algorithms (MD5, SHA-1) to be Used
- Defines Public Key Exchange to Use (RSA)

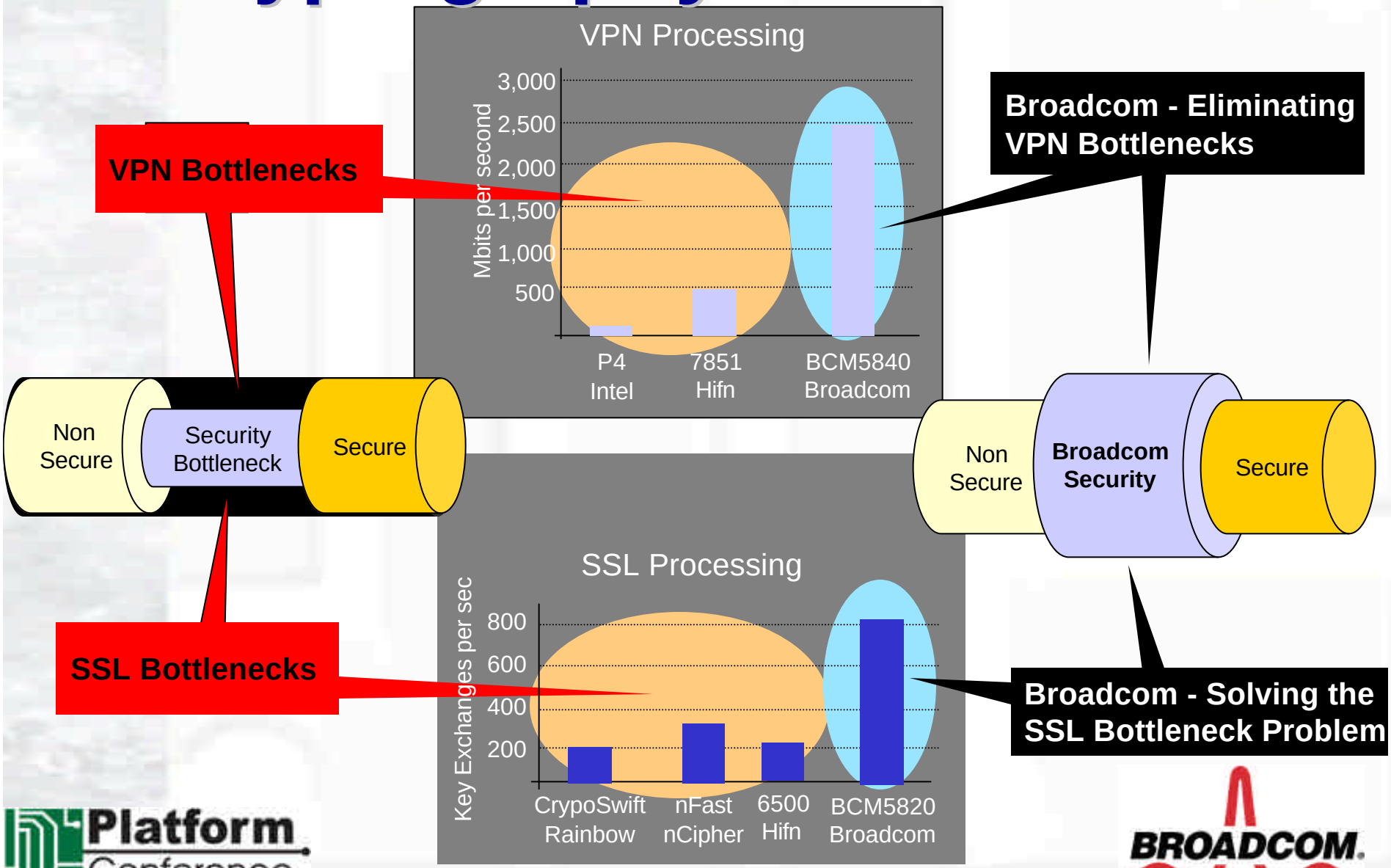
Modern Internet Security



Platform Conference

BROADCOM.

Cryptography Bottlenecks



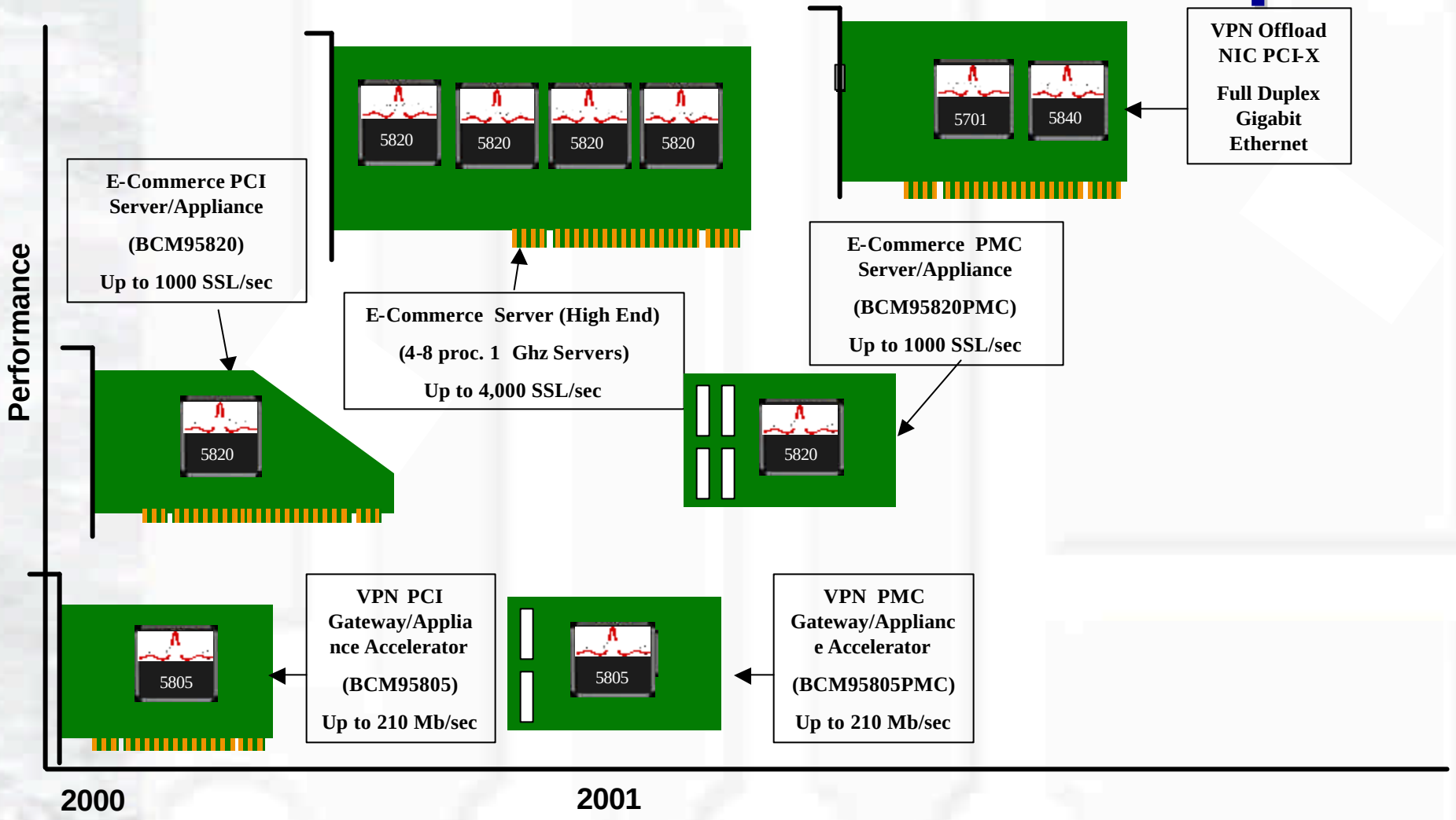
Platform Conference

BROADCOM.

E-Commerce and VPN Subsystems

- Benefits
  - Integrates with Tier 1 OS (Microsoft Win 2K, Check Point, Linux, Open SSL,)
  - Provide dramatic E-Commerce transaction rates with off the shelf Software and Server Hardware
  - Increase VPN performance to wirespeed data rates
  - Scalable architecture utilizing Broadcom Chips and Drivers
- Long-Term Performance Leader
  - Best SSL and VPN Products
  - Development and Integration with Leading Platforms' Next Generation Architectures

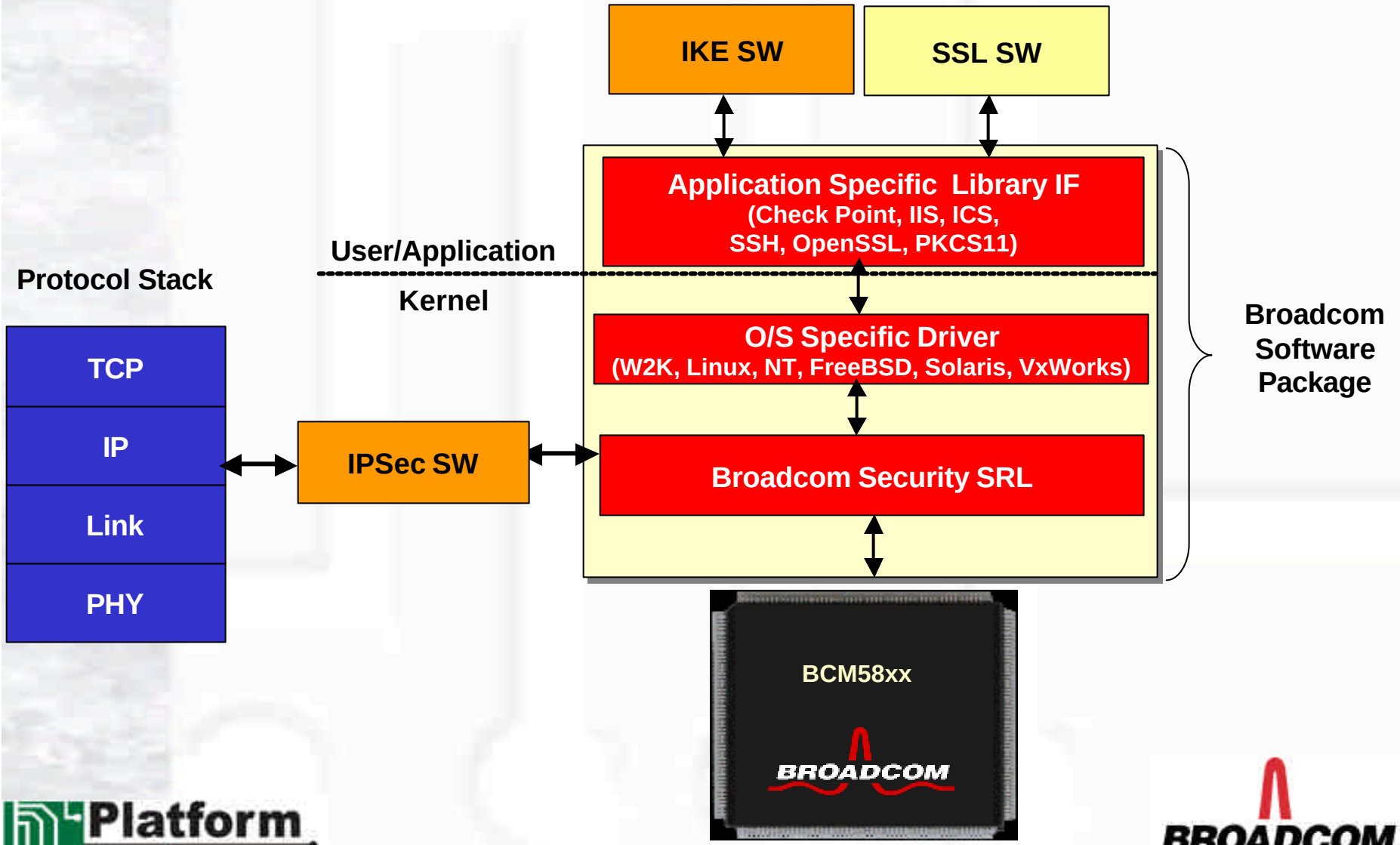
Reference Board Roadmap



Platform Conference

BROADCOM.

Software Drivers Solution



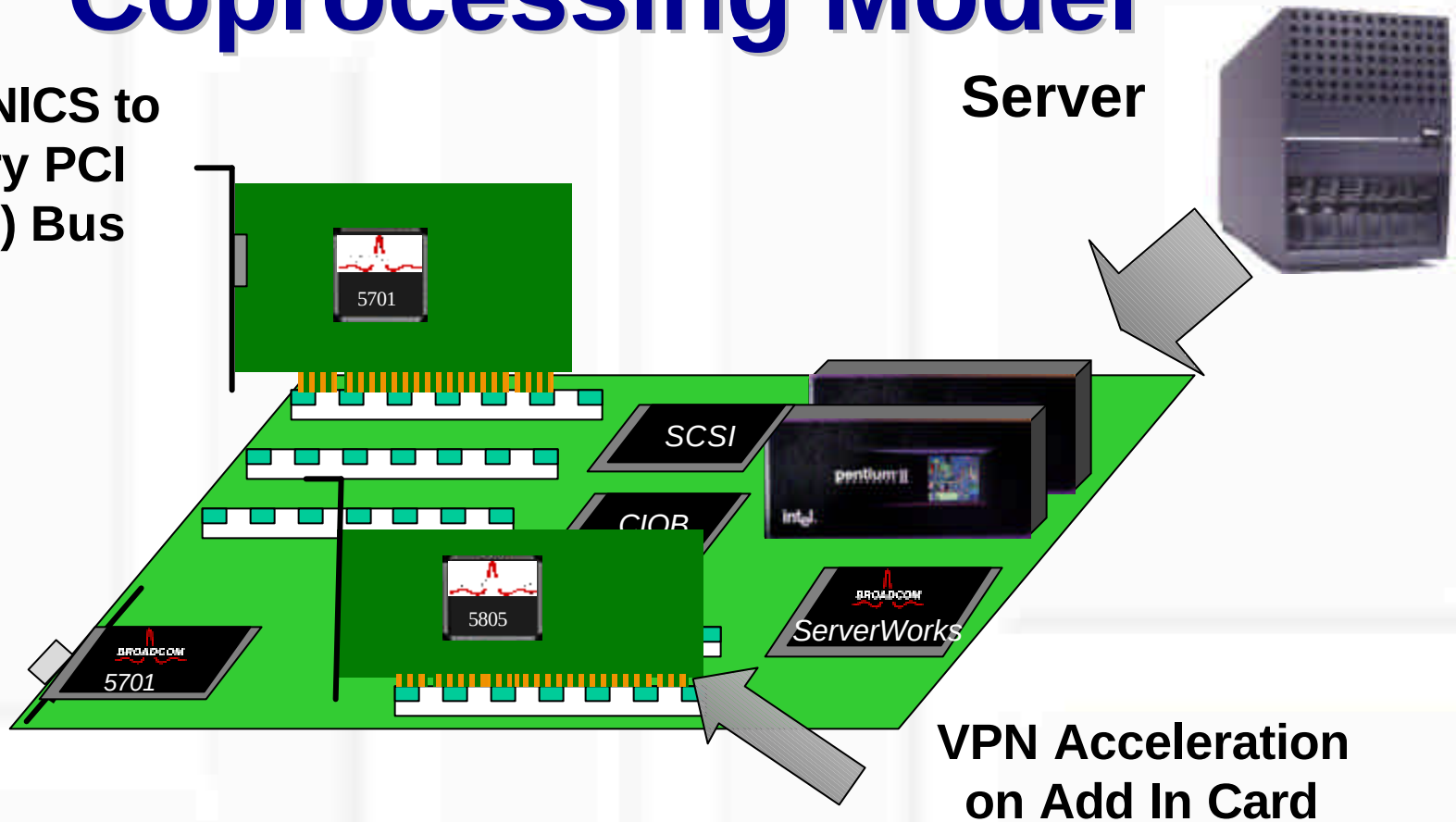
Platform Conference

BROADCOM.

Improving VPN Performance Coprocessing Model

Isolate NICS to primary PCI (PCI-X) Bus

Server



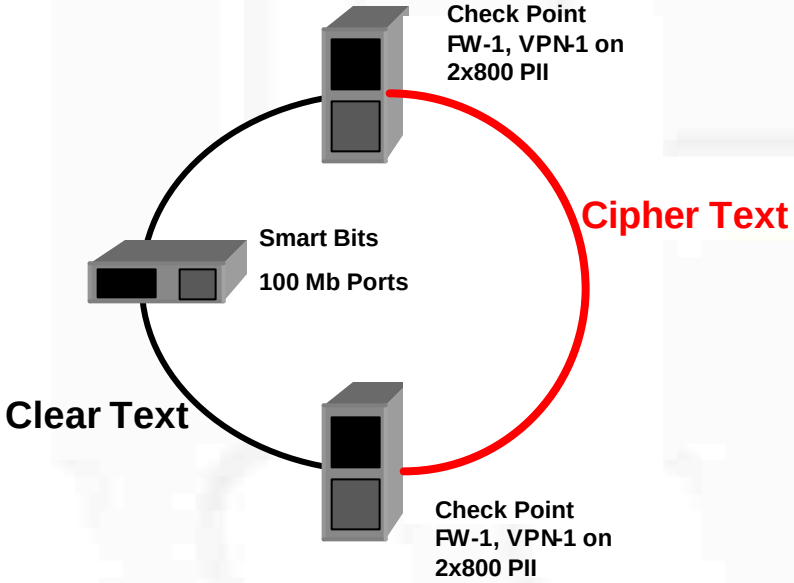
VPN Acceleration on Add In Card -e.g. Check Point -(2nd PCI Bus)

Platform Conference

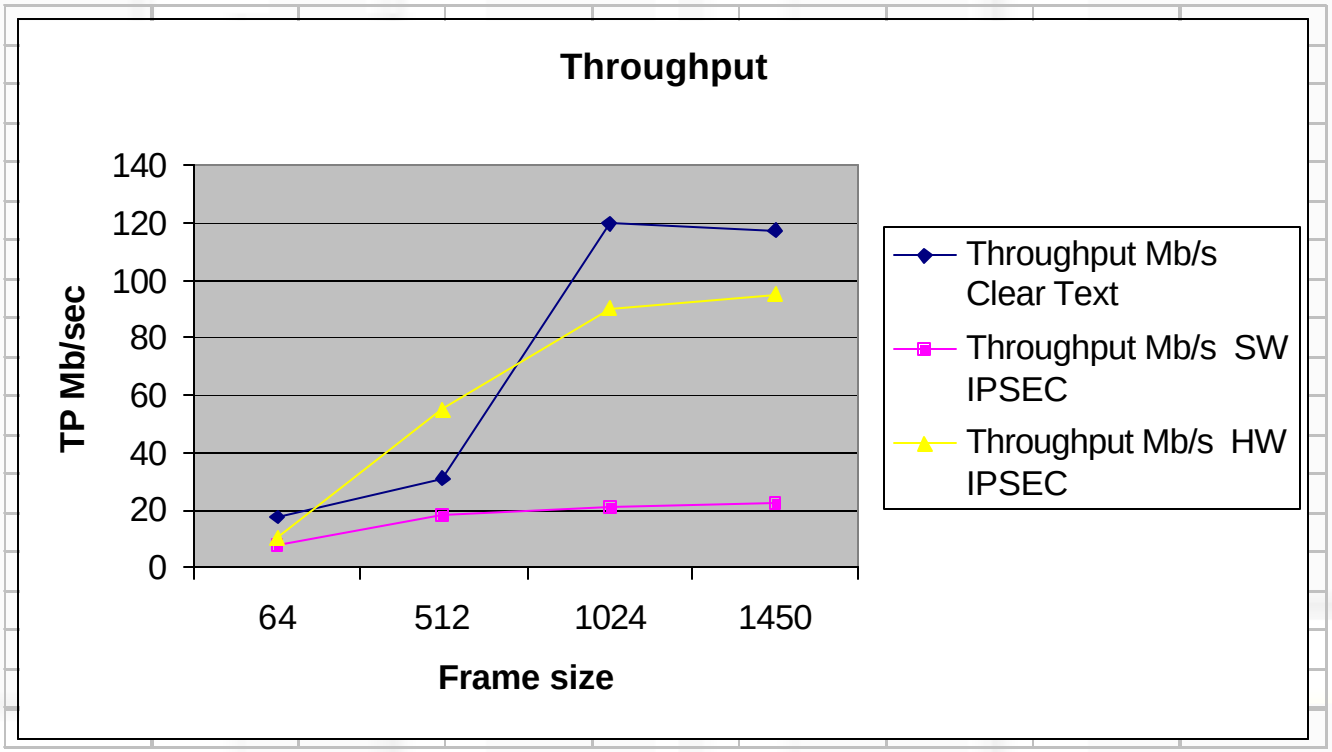
BROADCOM.

VPN Example

- Check Point VPN on Microsoft NT 4.0
  - NT to NT on 2 x 800 Mhz Pentium III
  - Sustaining 120 Mbs With HW Crypto
    - SW Performance 25 Mbs
  - BCM95805 Reference Design



Detailed IPsec Analysis

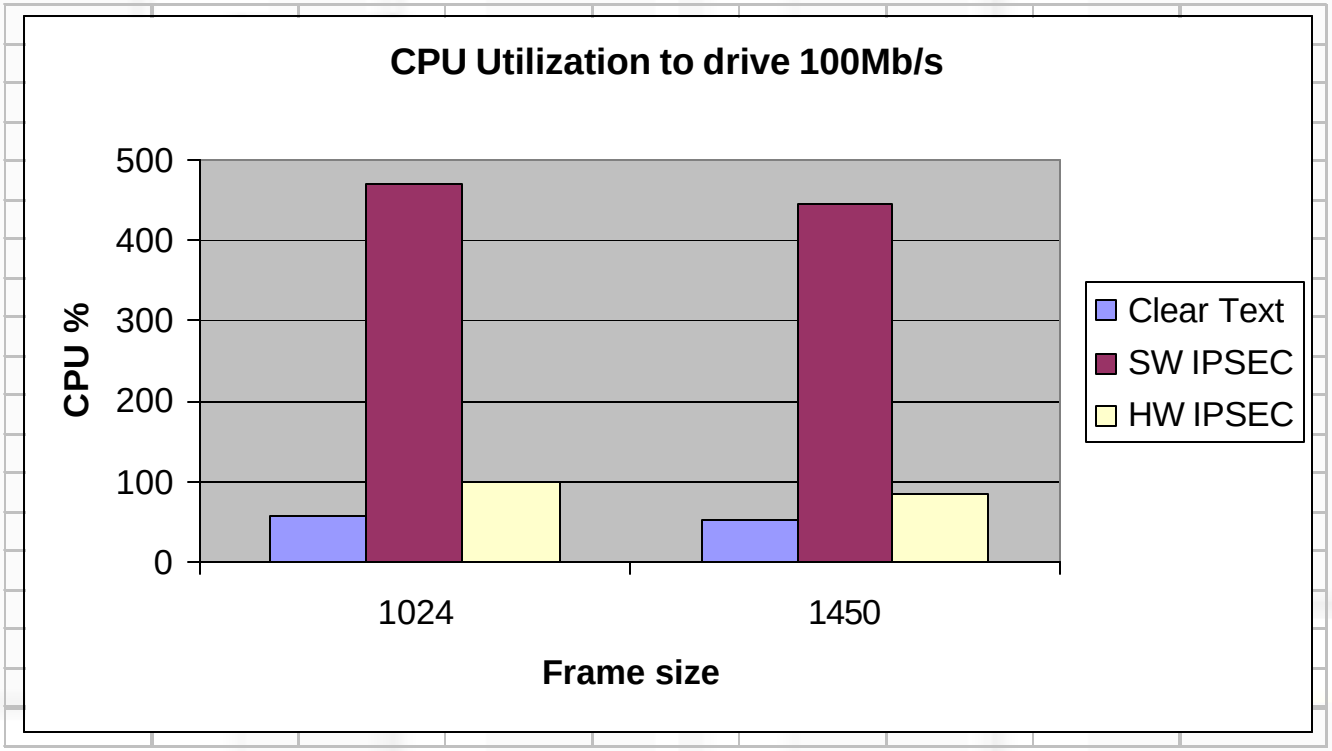


Single Processor 933Mhz PIII with 3rd Party Firewall IPsec Application on Windows 2K

Platform Conference

BROADCOM.

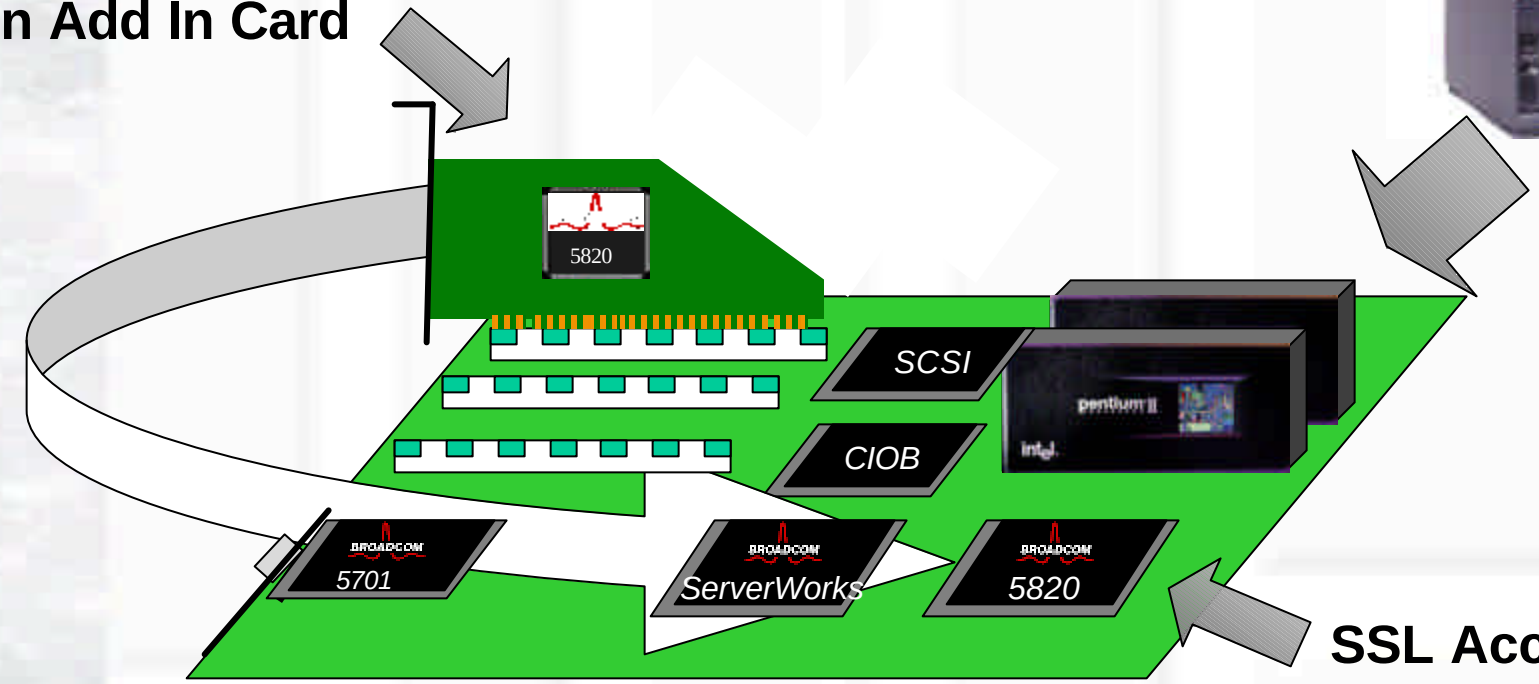
Detailed IPsec Analysis (Cont'd)



Single Processor 933Mhz PIII with 3rd Party IPsec and Firewall Application on Windows 2K

Options to Improve SSL Performance

SSL Acceleration on Add In Card



Server

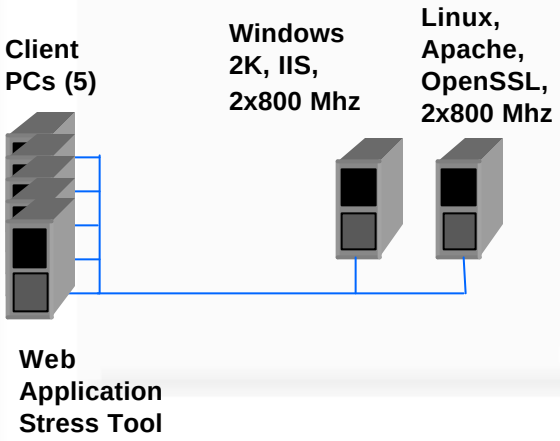
SSL Acceleration on Motherboard

Platform Conference

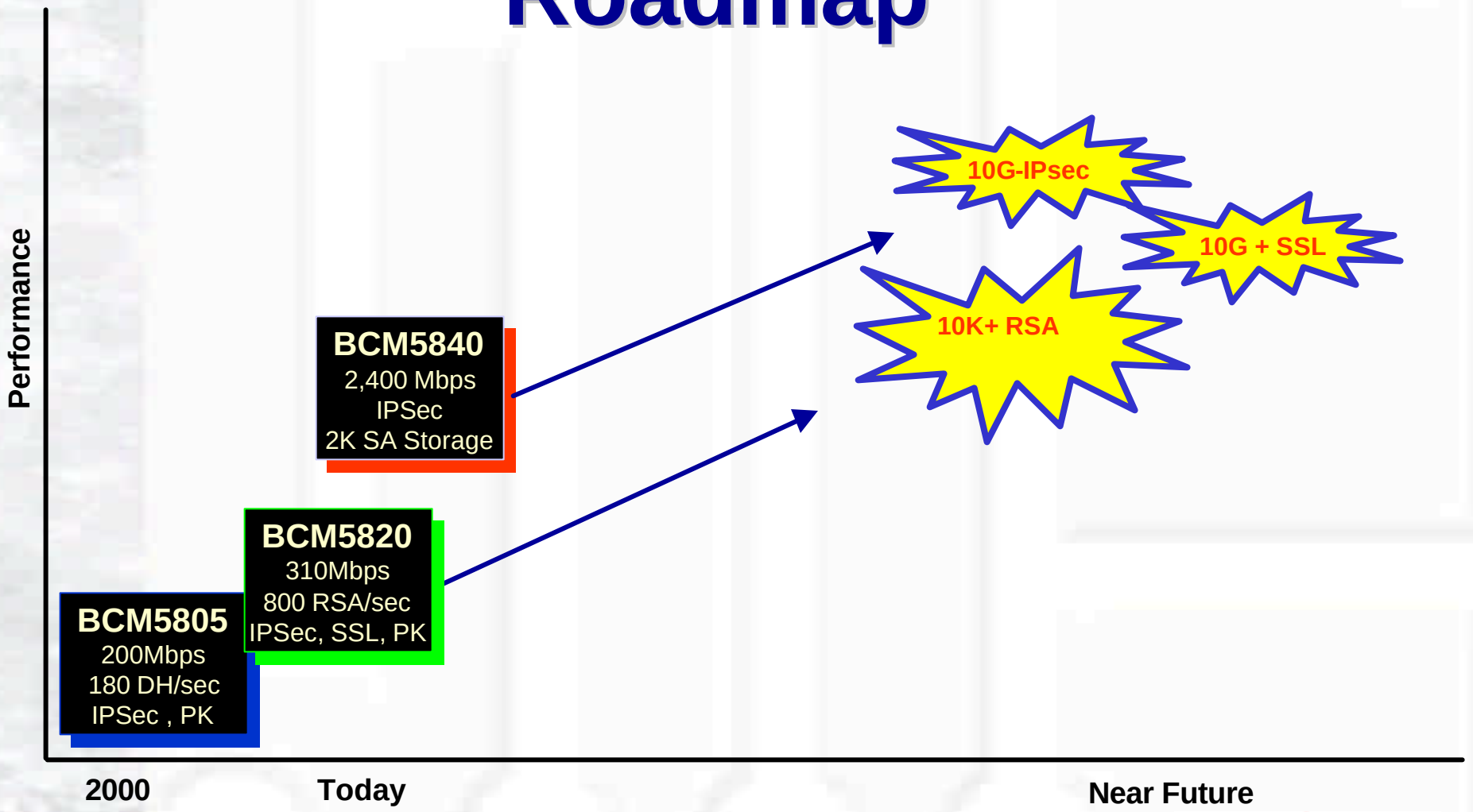
BROADCOM.

SSL Example

- Linux and Microsoft Win 2K
  - 2x800Mhz PIII
  - Complete Session Initiation and Tear Down
  - No Session Reuse, 1024 Bit Key Size
  - BCM95820
- Linux – OpenSSL with Apache
  - 749 Connections Per Second (CPS) with HW
    - 205 CPS with Software only
    - 860 RSA per second Raw Throughput
- Microsoft IIS - S-Channel Integration
  - 503 CPS with HW
    - 176 CPS with Software only



Cryptography Processing Roadmap



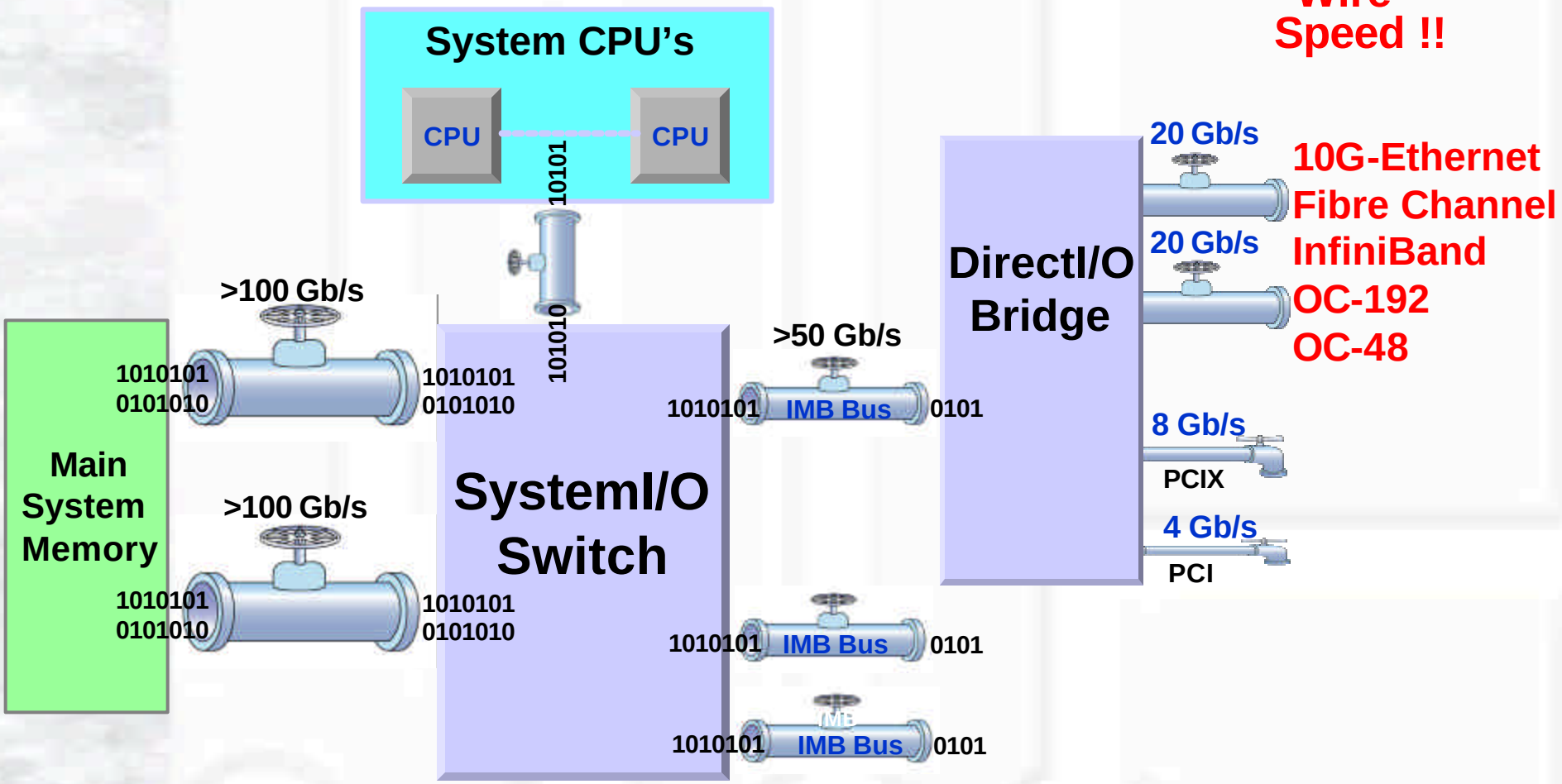
Platform Conference

BROADCOM.

ServerWorks Synergies

- Standard-setting technology for networking, servers
  - Over 120 Design Wins with Leading Manufacturers
  - Includes servers, network switches, storage applications
- Enabling technology for high performance cryptography systems
  - Direct interface into high speed system
  - Flexible system and I/O design

ServerWorks Synergies



Platform Conference

BROADCOM.

Summary

- Security Processing Hardware Becoming Mainstream
- Broadcom is Leading VPN System Level Performance
- Broadcom is Pushing Highest SSL Performance
- Broadcom is Leading the Market in Wirespeed Security Solutions for VPN and SSL
- Future Roadmap will Include Close Integration with ServerWorks and Broadcom Security LOB